

What is claimed is:

- 1 1. A key agreement method for secure communication in a multiple
2 access system, the key agreement method comprising the steps of:
3 (a) a first user encoding a signal from a source by a bit sequence and
4 transmitting the signal;
5 (b) a second user who is a legitimate counterpart of the first user decoding
6 the transmitted signal and measuring the decoded signal;
7 (c) the second user adopting only bits having the measured value beyond
8 the threshold value which is predetermined;
9 (d) the second user informing the first user that the bits adopted are the n-th
10 bits in the transmitted bit sequence, not telling the values of the bits; and
11 (e) the first and second users taking the adopted bits as a key string, and
12 discarding the remaining bits.

1 2. The method of claim 1, further comprising the steps of:
2 (f) selecting a subset of bits from the key string shared by the first and
3 second users and checking errors;
4 (g) if the error rate obtained in (f) is below a tolerable level, considering
5 the transmission safe, accepting the key string and obtaining a refined key string
6 with amplification such as error correction process; and
7 (h) discarding the key adopted in the step (e) if the error rate obtained in (f)
8 exceeds the tolerable level, returning to the step (a) and performing (a) through (f)
9 until getting the key string which satisfies the condition (g).

1 3. The method of claim 1, wherein the signal transmitted in the step (a)
2 is susceptible to noise.

1 4. The method of claim 1, wherein the second user uses a receiver
2 affected by mutual modulated noise by another transmitter.

1 5. The method of claim 1, wherein the threshold value of the step (c)
2 is determined by the second user considering at least a transmission rate, a
3 transmission error rate, and a degree of security.

1 6. The method of claim 4, wherein the threshold value of the step (c)
2 is determined by the second user considering at least a transmission rate, a
3 transmission error rate, and a degree of security.